UNITED STATES DISTRICT COURT
WESTERN DISTRICT OF WASHINGTON
AT SEATTLE

UNITED STATES OF AMERICA, Plaintiff, v. DOUGLAS BLOUIN, Defendant.	CR16-307 TSZ ORDER

THIS MATTER came before the Court on defendant Douglas Blouin's motion to compel discovery, docket no. 25. Having reviewed all papers filed in support of, and in opposition to, the motion, and having considered the oral arguments of counsel, the Court issued an oral ruling, granting the motion in part and denying the motion in part. *See* Minutes (docket no. 50). This Order incorporates by reference the Court's oral ruling and further explains the Court's reasoning.

Background

In the Superseding Indictment, defendant is charged with Attempted Receipt of Child Pornography, Receipt of Child Pornography, and Possession of Child Pornography. Superseding Indictment (docket no. 29). The charges are based on evidence the Government obtained using a software program known as RoundUp eMule, which is a law-enforcement developed version of a publicly-available ("open source") peer-to-peer

("P2P") file-sharing program known as eMule. *See* Erdely Decl. at ¶¶ 5 & 10 (docket no. 38-1). Both eMule and another program known as Shareaza operate in connection with the eDonkey/KAD P2P file-sharing network, which contains various servers that maintain indices of the files available on the network and the identities of the computers within the network that are sharing such files. *Id.* at ¶¶ 4-5. A user can search the eDonkey/KAD network to find the Internet Protocol ("IP") address of a computer that is sharing a file the user wants, and the user can then connect directly to such computer through eMule or Shareaza to download the file. *Id.* at ¶ 4. The system is analogous to looking up a person in a directory to find an associated telephone number and dialing the number to speak with the person. *Id.*

The parties do not dispute that, for someone to obtain a file via eMule or Shareaza from another person's computer, the file must be in the "share" folder of such computer at the time of the download request. *See id.* at ¶ 8. RoundUp eMule is likewise able to access files only if they are in the "share" folder of a computer in the eDonkey/KAD network. *See id.* at ¶¶ 12, 17, 21, & 23. Although eMule or Shareaza engage in multi-source downloading, thereby obtaining portions of each file from various computers to speed up the copying process, RoundUp eMule downloads files from a single source to ensure that they come from one particular eDonkey/KAD network user. *Id.* at ¶¶ 6 & 16.

RoundUp eMule runs searches to locate files with certain hash values that are associated with child pornography, which might take the form of a still image or a video. *Id.* at ¶ 13. These hash values are contained in a law enforcement database. *Id.* If RoundUp eMule finds one or more of these hash values at a particular IP address, the search results are entered into the "download candidate" database, which is available to all RoundUp eMule users. *Id.* The "download candidate" database provides leads or tips for investigators, which they can use to identify people sharing child pornography. *See id.* at ¶ 14.

According to the Government, Homeland Security Investigations Special Agent Toby Ledgerwood configured his version of RoundUp eMule to search in his geographic area of responsibility for eDonkey/KAD network users who were suspected of sharing child pornography. Via RoundUp eMule, Ledgerwood allegedly downloaded twelve videos and two images of child pornography from a computer with an IP address associated with defendant. After a search warrant was obtained, a Dell desktop computer was seized from defendant's home, on which both eMule and Shareaza were installed. A forensic examination of the computer revealed only one image of child pornography. According to Ledgerwood, during a recorded interview near the time of the search of his residence, defendant indicated that he had employed specialized software to "wipe" his computer and erase any remnants of child pornography. A forensic examination confirmed that the computer had been "thoroughly scrubbed" just days before the search.

Discussion

In his motion to compel, defendant sought the following evidence: (i) the law enforcement database of hash values associated with known child pornography; (ii) the "download candidate" database; (iii) the source code for the version of RoundUp eMule used in this matter; (iv) the network specifications, design documents, and user manuals for the version of RoundUp eMule used in this matter; and (v) the validation test results and related test specifications for the version of RoundUp eMule used in this matter. With regard to the latter two requests, the Government responded that no formal network specifications or design documentation exists for RoundUp eMule,[1] that a redacted copy of the user manual will be made available to the defense, and that no independent validation testing has been performed on the version of RoundUp eMule used in this matter, *see* Erdely Decl. at ¶ 3 (docket no. 48-1); Erdely Decl. at ¶ 31 (docket no. 38-1). The Court is satisfied that nothing further is required of the Government as to the fourth and fifth items, and thus, this Order addresses only the first three requests.

Federal Rule of Criminal Procedure 16 outlines the types of information the Government is required to disclose to defendant.[2] In particular, the Government must permit defendant to inspect and copy items in the Government's possession, custody, or control if (i) the item is "material" to preparing the defense; (ii) the Government intends

[1] At the Court's direction, the Government has filed a declaration confirming that it has no materials responsive to the fourth request, other than a user manual, which has already been provided to defense counsel. *See* Erderly Decl. at ¶ 3 (docket no. 54); *see also* Tr. (May 11, 2017) at 27:20 (docket no. 55) (defense counsel confirmed that he has a copy of the manual).

[2] Notwithstanding the provisions of Rule 16, the Adam Walsh Child Protection and Safety Act of 2006 ("Adam Walsh Act") precludes the Court from granting any request by defendant to "copy, photograph, duplicate, or otherwise reproduce" any material that constitutes child pornography, as long as the Government makes such material "reasonably available" to the defense. 18 U.S.C. § 3509(m)(2)(A). Material is deemed "reasonably available" if the Government provides "ample opportunity for inspection, viewing, and examination at a Government facility" by defense counsel and any defense expert. *Id.* at § 3509(m)(2)(B). Defendant attempts to use the Adam Walsh Act to require the Government to make the databases and source code at issue available for review at a Government facility. The Adam Walsh Act, however, does not apply to the items defendant seeks. The databases and source code are not themselves child pornography as defined in 18 U.S.C. § 2256(8); they are not "visual depictions" of "sexually explicit conduct" involving minors. Moreover, even if the Adam Walsh Act governed, it would not operate to broaden the scope of materials the Government must produce to defendant; defendant must still demonstrate that what he seeks falls within the bounds of Rule 16.

to use the item in its case-in-chief at trial; or (iii) the item was obtained from or belongs to defendant. Fed. R. Crim. P. 16(a)(1)(E). No assertion has been made that the entire hash value database, the entire "download candidate" database, or the source code for RoundUp eMule will be used as evidence in the Government's case-in-chief, and the items were undisputedly not procured from defendant. Thus, the only basis on which defendant seeks the databases and source code is their alleged materiality to preparing a defense. Defendant, however, has not made the requisite showing.

A. **Hash Values**

According to the Government, the hash value database contains millions of alpha-numeric sequences, each associated with a file known to contain child pornography. The only portion of the hash value database that is "material" in this matter is the small part associated with the fourteen files allegedly downloaded from defendant's computer. The Court is persuaded that defendant's first discovery request is overbroad, and that the Government is required to produce only the segment of the hash value database relevant to this matter. By oral ruling, the Court directed the Government to submit a declaration regarding whether the hash values for the twelve videos and two images downloaded in April 2016 allegedly from defendant's IP address were among the hash values in the law enforcement database. *See* Minutes (docket no. 50). The Government has since filed a declaration indicating that defense counsel has been given a spreadsheet listing the fourteen hash values at issue and the date on which each hash value was added to the database. *See* Erdely Decl. at ¶¶ 1-2 (docket no. 54). Defendant has not demonstrated that he is entitled to anything further.

B. <u>"Download Candidate" Database</u>

The "download candidate" database also contains much more information than is "material" to preparing a defense in this case. Defense counsel has already been provided the results of a search of the "download candidate" database for all instances in which defendant's IP address appears or is considered a "download candidate." *See* Erdely Decl. at ¶ 30 (docket no. 38-1). Defendant offers no explanation for why the Government should be required to divulge to him, his attorney, or his expert the leads or tips that law enforcement might have concerning other individuals suspected of sharing child pornography.

C. <u>Source Code</u>

In support of his motion to compel the Government to produce the source code for the version of RoundUp eMule used in this matter, defendant cites *United States v. Budziak*, 697 F.3d 1105 (9th Cir. 2012). *Budziak* does not support defendant's position.[3] In *Budziak*, the Ninth Circuit concluded that the district court erred in denying the defendant's request for disclosure of the source code and technical specifications for the

[3] Defendant's reliance on *United States v. Soto-Zuniga*, 837 F.3d 992 (9th Cir. 2016), is equally misplaced. In *Soto-Zuniga*, the Ninth Circuit held that the district court abused its discretion in denying discovery of search and arrest statistics for the San Clemente, California checkpoint. *Id.* at 998-1002. The Ninth Circuit considered those statistics "material" to the issue of whether the San Clemente checkpoint continued to serve the purpose of immigration control, which had previously been approved, despite a Fourth Amendment challenge, as the basis for stopping cars and posing questions without individualized suspicion of wrongdoing. *Id.* at 999-1000; *see id.* at 1002 ("Whether the primary purpose of the checkpoint has evolved from controlling immigration to detecting 'ordinary criminal wrongdoing' is a question that is subject to discovery under Rule 16." (citation omitted)). Search and arrest statistics are substantially different from source code, and unlike the defendant in *Soto-Zuniga*, defendant in this case has not made the requisite showing that the source code for RoundUp eMule would assist him in challenging the search and/or seizure at issue.

Federal Bureau of Investigation ("FBI") computer program called EP2P, which was an enhanced version of LimeWire, another P2P file-sharing program. 697 F.3d at 1107, 1112-13. In *Budziak*, the defendant presented evidence suggesting that the FBI, by using EP2P, downloaded only fragments of child pornography files from his computer, raising doubt about whether he knowingly distributed complete child pornography files, and that FBI agents could have used EP2P to override or alter the defendant's sharing settings in LimeWire. *Id.* at 1112. In this matter, defendant makes no similar showing. Defendant does not dispute that RoundUp eMule downloads only from a single source, and he does not allege that either eMule or Shareaza, like LimeWire, allows a user (or a connecting "peer," *e.g.*, a law enforcement agent) to modify the sharing settings.[4]

This case is similar to *United States v. Pirosko*, 787 F.3d 358 (6th Cir. 2015), in which the defendant failed to produce any evidence of governmental wrongdoing and, as a result, the district court's denial of a similar motion to compel disclosure of the source code for the surveillance program ShareazaLE was affirmed. The Court adopts the reasoning set forth in *Pirosko*, and concludes that, with respect to the source code for RoundUp eMule, defendant has not met the standard for disclosure set forth in Rule 16. The Court is also persuaded that granting defendant's request for the source code would "compromise the integrity of [the government's] surveillance system and would frustrate future surveillance efforts." *See id.* at 365.

[4] The Government acknowledges that a Shareaza user like defendant could configure the program to inhibit file sharing with others on the eDonkey/KAD network. *See* Erdely Decl. at 7 n.3 (docket no. 38-1). Even if defendant had attempted to configure his Shareaza program to prevent file sharing, such fact would not implicate RoundUp eMule or justify disclosure of its source code.

Conclusion

For the foregoing reasons, defendant’s motion to compel discovery, docket no. 25, was granted in part and denied in part.

IT IS SO ORDERED.

Dated this 14th day of June, 2017.

Thomas S Zilly

Thomas S. Zilly
United States District Judge